Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 369 BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 oktober 2015

Hierbij bied ik uw Kamer, vanuit mijn coördinerende verantwoordelijkheid voor cybersecurity, de vijfde editie van het Cyber Security Beeld Nederland 2015 (CSBN 2015) aan[1]. Tevens informeer ik u over de voortgang van de implementatie van het werkprogramma bij de Nationale Cyber Security Strategie 2 (NCSS 2) en de uitkomsten van het onderzoek naar de effectiviteit van de adviesproducten van het NCSC door de Inspectie Veiligheid en Justitie.
Het CSBN wordt jaarlijks met partners vanuit de publieke sector, de private sector en wetenschap, onder de verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), opgesteld door het Nationaal Cyber Security Centrum (NCSC). Het doel is het bieden van inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity over de periode april 2014 tot en met april 2015. Het CSBN vormt een belangrijk uitgangspunt en referentiekader voor de NCSS 2 en de speerpunten uit het daaraan gekoppelde actieprogramma. Het actieprogramma van de NCSS 2 kent 10 speerpunten en 37 actiepunten die door middel van publiek-private samenwerking worden gerealiseerd. In bijlage 1 informeer ik u aan de hand van de speerpunten over de voortgang van het actieprogramma.
De kernbevindingen, conclusies en beleidsopvolging zijn besproken in de Cyber Security Raad.

Het CSBN 2015 (zoals gevoegd in bijlage 2) laat zien dat eerder gesignaleerde trends in voorgaande cybersecuritybeelden zich doorzetten. Cybercrime en digitale spionage blijven de grootste dreiging. Geopolitieke ontwikkelingen hebben daarbij een belangrijke invloed op de ontwikkeling van de dreiging. Sinds het verschijnen van de NCSS 2 in 2013 is de internationale veiligheidsomgeving voor Nederland veranderd, zoals beschreven in de «Beleidsbrief Internationale Veiligheid -Turbulente Tijden

[1] Raadpleegbaar via www.tweedekamer.nl

kst-26643-369
ISSN 0921 - 7371
’s-Gravenhage 2015

in een Instabiele Omgeving»[2], die op 14 november 2014 door de Minister van Buitenlandse Zaken aan uw Kamer is gezonden. De daarin geschetste ontwikkelingen raken ook het digitale domein. In het CSBN 2015 wordt dit ook nadrukkelijk geconstateerd als een van de kernbevindingen:

1. *Criminelen zetten cryptoware (gijzelvirussen) steeds vaker in om hun doeleinden te bereiken.*
   In tegenstelling tot andere veel voorkomende malware, zoals Remote Access Tools (RAT's), blokkeren de criminelen hier de toegang tot gegevens met behulp van encryptie. De bereidheid van mensen en organisaties om de criminelen te betalen zorgt voor hoge gemiddelde opbrengsten per doelwit voor criminelen. Geavanceerdere vormen, bijvoorbeeld gericht op het ontoegankelijk maken van webapplicaties in plaats van alleen pc's, zijn inmiddels waargenomen.
2. *Geopolitieke spanningen manifesteren zich steeds vaker in (dreigende) inbreuken op digitale veiligheid.*
   Staten en andere actoren die in lijn met het belang van deze staten lijken te acteren maken steeds vaker gebruik van digitale aanvallen om hun belangen te behartigen en daarmee geopolitieke verhoudingen of ontwikkelingen te beïnvloeden. Digitale aanvallen zijn een aantrekkelijk alternatief voor en aanvulling op conventionele militaire en spionagemiddelen vanwege de grote impact tegen lage kosten en afbreukrisico's. Conflicten, aanslagen of politieke gevoeligheden zijn het afgelopen jaar veelvuldig aanleiding geweest voor digitale aanvallen.
3. *Phishing wordt veel gebruikt in gerichte aanvallen en is dan voor gebruikers nauwelijks te herkennen.*
   Phishing (het «vissen» naar inlog- en andere gegevens van gebruikers) speelt een sleutelrol bij het uitvoeren van gerichte digitale aanvallen en blijft een laagdrempelige en effectieve aanvalsmethode. Phishingmails in gerichte aanvallen zijn voor gebruikers in veel gevallen nauwelijks te herkennen als niet-authentiek. Met behulp van een geslaagde phishingcampagne weten aanvallers toegang te krijgen tot interne netwerken van organisaties en de daar opgeslagen informatie. Technische middelen om authentieke e-mail als zodanig herkenbaar te maken worden in de praktijk slechts beperkt toegepast.
4. *Beschikbaarheid wordt belangrijker nu alternatieven voor ICT-systemen verdwijnen.*
   Belangrijke maatschappelijke processen komen tot stilstand als de bijbehorende ICT-systemen en analoge alternatieven niet beschikbaar zijn. Het verdwijnen van analoge alternatieven voor ICT-systemen maakt de beschikbaarheid van deze systemen daarom nog belangrijker. Dit is vooral het geval waar deze ICT-systemen belangrijke maatschappelijke processen als transport, financieel verkeer of energievoorziening ondersteunen. De maatregelen die banken hebben getroffen tegen DDoS-aanvallen tonen aan dat het mogelijk is effectieve maatregelen te treffen om beschikbaarheid van digitale voorzieningen te verhogen. Organisaties treffen dergelijke maatregelen echter vaak pas als de ICT-systemen al beschikbaarheidsproblemen hebben gekend.
5. *Kwetsbaarheden in software zijn nog altijd de achilleshiel van digitale veiligheid.*
   Software is een cruciaal onderdeel van onze digitale infrastructuur omdat software de mogelijkheden van hardware en de steeds groeiende hoeveelheid data ontsluit. Ook dit jaar hebben softwareleveranciers duizenden updates uitgebracht om kwetsbaarheden in hun software te repareren. De belemmeringen die organisaties ervaren bij het installeren van updates zorgen ervoor dat ze het installeren ervan soms achterwege laten. Zo lang de updates niet geïnstalleerd zijn blijven delen van hun netwerk kwetsbaar. Actoren die bijvoorbeeld via

[2] Kamerstuk 33 694, nr. 6

phishing of zero-day kwetsbaarheden binnendringen weten zich door zulke kwetsbaarheden verder door het netwerk te bewegen.
Met de toenemende toepassing van software op nieuwe plaatsen, zoals medische apparatuur of als onderdeel van het Internet der Dingen, neemt het belang van veiligheid verder toe. Helaas blijkt de software in deze apparaten regelmatig elementaire kwetsbaarheden te bevatten. Updates, die vaak handmatig geïnstalleerd moeten worden zijn door de aard van deze apparaten niet eenvoudig te installeren.

Conclusies CSBN en beleidsopvolging

Deze kernbevindingen bevestigen de noodzaak tot een integrale, publiek-private, (inter)nationale cybersecurity-aanpak, zoals ingezet met de NCSS 2. In aanvulling daarop zullen de volgende initiatieven worden geïnitieerd.

Aanvullende aandacht voor phishing en cryptoware

In de campagne Alert Online, die loopt van 26 oktober tot 6 november 2015, zal samen met publieke en private partners aanvullende aandacht worden besteed aan manifestaties van cybercrime die burgers en bedrijven gericht treffen, zoals phishing en cryptoware. Daarnaast zal het NCSC nog in het najaar van 2015 de technische normen en standaarden om phishing tegen te gaan breed onder de aandacht brengen.

Versterken samenspel veiligheidsorganisaties in digitale domein

Het samenspel van veiligheidsorganisaties in het digitale domein zal verder worden versterkt. Een geïntegreerde aanpak waarbij nationale capaciteiten, netwerken en samenwerkingsverbanden publiek-privaat en civiel-militair worden uitgebouwd en bestendigd is noodzakelijk. Deze partijen kennen een grote wederzijdse afhankelijkheid en kunnen daardoor alleen samen de dreiging effectief aanpakken. Hierdoor ontstaan robuuste netwerken die meegroeien in het licht van de veranderende dreiging. In dat verband is het van belang om het Nationaal Detectie Netwerk (NDN), een samenwerkingsverband van NCSC, AIVD en MIVD verder op en uit te bouwen zodat geavanceerde dreigingen tijdig gedetecteerd kunnen worden en een tijdige en effectieve respons kan worden gerealiseerd. Daarnaast is het, in het licht van de huidige geopolitieke situatie, van belang om inzicht in de digitale capaciteiten, intenties en activiteiten van (statelijke) actoren te krijgen. Dit inzicht is randvoorwaardelijk voor de weerbaarheid verhogende maatregelen van de veiligheidsorganisaties.

Doorontwikkeling adviesproducten NCSC

De Inspectie Veiligheid en Justitie heeft in 2015 een onderzoek gedaan naar het gebruik van beveiligingsadviezen van het NCSC (bijlage 3)[3]. Uit het onderzoek blijkt dat alle organisaties de beveiligingsadviezen van het NCSC lezen, beoordelen en indien nodig de noodzakelijke maatregelen treffen. Betrokken partijen waarderen de kennis en expertise van het NCSC. Dit betreft niet alleen de beveiligingsadviezen, maar ook de andere producten die het NCSC levert (bijvoorbeeld factsheets, white papers en sectorale overlegvormen). De Inspectie concludeert dat de beveiligingsadviezen in de huidige vorm beperkte meerwaarde hebben. De Inspectie onderschrijft de ambitie van het NCSC om haar capaciteiten zo efficiënt en effectief mogelijk in te zetten. In dat kader beveelt de Inspectie het NCSC aan om het product beveiligingsadviezen te heroverwegen.

[3] Raadpleegbaar via www.tweedekamer.nl

Het rapport van de Inspectie verwelkom ik van harte. De bevindingen worden binnen het NCSC herkend. De verbeterpunten worden thans opgepakt.

Internationale aanpak als integraal onderdeel van cybersecurity

Cybersecurityvraagstukken zijn grensoverschrijdend. Het CSBN 2015 illustreert dit wederom. Internationale samenwerking is van cruciaal belang voor de cybersecurity van Nederland. Dit was een belangrijke reden voor Nederland om gastheer te worden van de Global Conference on Cyberspace 2015 (GCCS2015) op 16 en 17 april dit jaar.

Nederland zal samen met alle stakeholders blijven werken aan een *internet governance* model dat een vrij, open en veilig internet garandeert. In het licht van de verslechterde internationale veiligheidssituatie en voortbouwend op de resultaten van GCCS2015 zal Nederland blijven werken aan het bewerkstelligen van een internationaal normatief kader voor de regulering van cyberoperaties tussen staten. Bovendien werkt Nederland aan het versterken van de opsporing van criminelen in cyberspace door hechtere internationale samenwerking en het zoeken naar oplossingen voor jurisdictievraagstukken. Daarnaast zal de lijn op internetvrijheid worden voortgezet, met een bijzondere inzet op het versterken van de rol van mensenrechten en het multistakeholdermodel in cyber besluitvormingsprocessen. Ook capaciteitsopbouw in derde landen blijft een prioriteit die wordt uitgewerkt in het kader van het tijdens de GCCS2015 opgerichte Global Forum on Cyber Expertise (GFCE) waarvan het secretariaat in Nederland is gevestigd. Tevens wordt de kabinetsreactie op de adviezen van de Adviesraad Internationale Vraagstukken en de Wetenschappelijke Raad voor het Regeringsbeleid over internationaal internetbeleid dit najaar aan uw Kamer aangeboden.

Het voorgaande illustreert de sterke nationale en internationale verwevenheid van de verschillende aspecten van cyberspace. Of het nu gaat om standaarden in ICT, fundamentele rechten, de bestrijding van cybercrime of het bevorderen van de internationale rechtsorde in cyberspace, een internationale beleidsagenda is belangrijk onderdeel van een geïntegreerd nationaal cybersecuritybeleid.

Doorontwikkeling Nederlandse cybersecurity aanpak

Naast bovengenoemde directe acties is een structurele doorontwikkeling van de Nederlandse cyberaanpak, die in lijn is met de ontwikkeling van de dreiging, nodig. De ontwikkeling van cyberdreigingen in combinatie met een instabieler wordende geopolitieke omgeving en toenemende afhankelijkheid van ICT vragen om structurele aandacht en een doorontwikkeling van de aanpak en capaciteiten om de Nederlandse digitale weerbaarheid te versterken. Dit vindt op dit moment plaats in het kader van het actieprogramma (2014–2016) van de NCSS 2. De implementatie van het actieprogramma ligt op schema en voorziet Nederland van een stevige basis.

Het digitale domein is een dynamisch domein waarbij technische en maatschappelijke ontwikkelingen snel gaan en de dreiging snel evolueert. Om in te spelen op deze nieuwe ontwikkelingen zal vanaf 2016 een doorontwikkeling van de cybersecurity visie moeten plaatsvinden en een geactualiseerde, en daar waar nodig, geïntensiveerde aanpak. De Nederlandse visie is en blijft dat in onze steeds belangrijker wordende digitale samenleving telkens de optimale balans tussen vrijheid, veiligheid en economische groei moet worden gevonden. De doorontwikkeling zal, net als bij de totstandkoming van de NCSS2, worden vormgegeven met

publieke en private stakeholders om te komen tot een gedragen Nederlandse cybersecurity aanpak in het mondiale digitale domein voor 2017 en verder.

Afsluitend

De uitwerking van het actieprogramma van de NCSS 2 krijgt vorm. De acties uit het actieprogramma naderen hun voltooiing door middel van de actieve inzet van betrokken publieke en private partijen. Hiermee zijn belangrijke stappen gezet om de weerbaarheid van Nederland te versterken. Het CSBN 2015 laat zien dat de in voorgaande cybersecurity beelden geconstateerde trends en ontwikkelingen zich versterkt doorzetten in 2015. Dit bevestigt het belang van de met de NCSS 2 ingeslagen weg. Het kabinet investeert daarom ook de komende jaren onverminderd in cybersecurity, via publiek-private participatie, samen met kennisinstellingen en vitale processen. Internationale samenwerking is daarbij van belang. Tijdens het Nederlandse EU voorzitterschap zal Nederland haar aanpak op dit terrein nadrukkelijk agenderen. De thema's cybersecurity, cybercrime, cyberdiplomatie en capaciteitsopbouw zullen speerpunten zijn van het Nederlandse EU voorzitterschap.

Met het CSBN en in het Nationaal Cyber Security Centrum van de NCTV worden de ontwikkelingen in het digitale domein nauwlettend gevolgd zodat, wanneer dat nodig is naar aanleiding van technische of maatschappelijke ontwikkelingen, acties aangescherpt of geïntensiveerd worden en actief kan worden ingespeeld op ontwikkelingen.

De Staatssecretaris van Veiligheid en Justitie,
K.H.D.M. Dijkhoff

Bijlage 1

Voortgang speerpunten Nederlandse cybersecurity aanpak

De Nationale Cyber Security Strategie 2 (NCSS 2) kent 5 doelstellingen, namelijk Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het digitale domein, Nederland pakt cybercrime aan, Nederland investeert in veilige en privacy bevorderende ICT producten en diensten, Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het digitale domein en Nederland beschikt over voldoende cybersecurity-kennis en -kunde en investeert in ICT-innovatie om onze cybersecurity-doelstellingen te behalen. Ter verder uitwerking van deze 5 doelstellingen zijn tien speerpunten benoemd. In deze bijlage wordt de voortgang op de NCSS 2 toegelicht aan de hand van deze 10 speerpunten.

Aanpak vitaal: risicoanalyses, veiligheidseisen en informatiedeling

De vitale infrastructuur is cruciaal voor het goed functioneren van onze samenleving. Onder vitale infrastructuur verstaan we producten, diensten en de onderliggende processen die, als zij uitvallen, maatschappelijke ontwrichting kunnen veroorzaken. Het is daarom belangrijk om deze vitale processen en objecten te beschermen tegen uitval door storingen, rampen, sabotage of aanslagen. Om het beschermingsniveau van de vitale infrastructuur in Nederland hoog te houden, werken overheid en bedrijfsleven samen aan het verder verbeteren van continuïteit en security door meer focus en samenhang aan te brengen. Daarom heeft in 2014 een «herijking» van de vitale sectoren plaatsgevonden. Doel van deze herijking was om een actuele lijst van vitale diensten en processen te definiëren, die basis vormt voor samenhang en prioriteitsstelling van verdere verhoging van de weerbaarheid van vitale processen. In het kader van de aanpak voor de bescherming van de vitale infrastructuur brengt de overheid samen met vitale partijen in beeld welke ICT-afhankelijke systemen, diensten en processen vitaal zijn. De samenhang tussen fysieke security en cybersecurity is daarbij een bijzonder aandachtspunt. Er is een lijst met 22 vitale processen opgesteld, met een aantal processen nog in onderzoek. Uw Kamer is hierover d.d. 12 mei jl. reeds geïnformeerd.[4]

Haalbaarheidsonderzoek gescheiden netwerk vitaal

In 2014 is in publiek-privaat verband een verkenning uitgevoerd naar een gescheiden ICT-netwerk voor (publieke en private) vitale processen. De verkenning geeft enerzijds inzicht in het feit dat een volledig gescheiden netwerk of het gesloten maken van delen van het internet op zichzelf geen realistische opties zijn. Het open karakter is de intrinsieke waarde die het internet vertegenwoordigt. Anderzijds wordt geconcludeerd dat de onderliggende belangen: beschikbaarheid, integriteit en vertrouwelijkheid blijvend beschermd dienen te worden. Dit kan betekenen dat op basis van een uitvoerige risicoanalyse door eigenaren van informatiesystemen wordt besloten tot het creëren van een veilige omgeving middels bij de situatie passende (scheidings-) maatregelen, zoals o.a. ook plaatsvindt binnen de rijksoverheid door fysieke en/of virtuele scheiding van specifieke netwerkvoorzieningen. Voor een nadere toelichting op de bevindingen van dit haalbaarheidsonderzoek verwijs ik uw Kamer naar mijn brief van 24 november 2014[5] waarin ik uw Kamer over de bevindingen van deze verkenning heb geïnformeerd. In deze brief is tevens aangegeven dat het NCSC een faciliterende rol speelt bij publiek-private en private initiatieven die bijdragen aan het verhogen van de weerbaarheid op dit vlak. Deze lijn wordt in 2016 verder doorgezet.

---

[4] Kamerstuk 30 821, nr. 23
[5] Kamerstuk 26 643, nr. 337

Gedragen standaarden en security en privacy by design

Veel oudere ICT systemen die thans in gebruik zijn, waren niet altijd ontwikkeld met privacy en veiligheid in gedachte. Om op de lange termijn over veiligere ICT-systemen te kunnen beschikken, zet het kabinet in op het stimuleren van de ontwikkeling en aanschaf van veilige hard- en software. Het belang van aantoonbaar veilig ontwikkelde software is in de voortgangsbrief Visie Telecom, Media en Internet en de Nationale Cyber Security Strategie geduid. Om dit te realiseren hebben diverse marktpartijen, w.o. Security Academy en iComply, gewerkt aan een nieuw «Normenkader Secure Software», in nauwe samenwerking met het Ministerie van Economische zaken en ECP. De eerste versie van het normenkader is met succes getest bij diverse software- ontwikkelorganisaties. Het normenkader legt een basis onder «veilig programmeren» en richt zich op alle belanghebbenden in de softwareketen die baat hebben bij duidelijke en objectief meetbare veiligheidskenmerken van software. Opdrachtgevers krijgen met dit normenkader de mogelijkheid om veilige software in hun lijst van vereisten op te nemen; ontwerpers en ontwikkelaars kunnen er gebruik van maken bij het bouwen van applicaties. Bedrijven krijgen hiermee de mogelijkheid om software te certificeren op veiligheid. De verdere ontwikkeling wordt vormgegeven door organisaties en bedrijven binnen een onafhankelijke stichting in oprichting: de Secure Software Foundation (i.o.).

Voorts is in 2014 een publiek privaat platform internetstandaarden ingericht om de toepassing van moderne internetstandaarden te stimuleren. Zowel de betrokken partijen die internetstandaarden ontwikkelen als de partijen die deze moeten implementeren nemen plaats in dit platform. Een website van het platform, internet.nl, is tijdens de GCCS2015 gelanceerd.

Versterkte aanpak cyberspionage

Cyberspionage blijft één van de twee grootste cyberdreigingen waarmee Nederland wordt geconfronteerd die zich voortdurend ontwikkelt. De aanpak van de dreiging die uitgaat van cyberspionage kent een toegenomen urgentie in het licht van de verslechterde internationale veiligheidssituatie. De frequentie, complexiteit en impact van deze aanvallen blijft toenemen. De jaarverslagen van de inlichtingen- en veiligheidsdiensten en het CSBN bevestigen deze trend. Nederlandse instellingen binnen en buiten de overheid zijn in toenemende mate het doelwit van digitale spionageactiviteiten. Deze ontwikkelingen vragen om een constante aanscherping van de inspanningen om adequaat op deze dreiging te reageren. In het actieprogramma van de NCSS 2 uit 2013 is voorzien in een versterking van de onderzoeks- en analysecapaciteiten van de Algemene Inlichtingen en Veiligheidsdienst (AIVD), Militaire Inlichtingen en Veiligheidsdienst (MIVD) en het Nationaal Cyber Security Centrum (NCSC) om de toen reeds grote dreiging van cyberspionage aan te pakken. In 2014 is in dit kader de Joint Sigint Cyber Unit (JSCU) van de AIVD en MIVD gerealiseerd en zijn de onderzoeks- en analysecapaciteiten van de AIVD en de MIVD versterkt. Ook wordt verkend hoe de samenwerking tussen deze partijen kan worden versterkt op het gebied van informatiedeling over digitale aanvallen en gezamenlijke analyses, binnen de geldende juridische kaders. Ten aanzien van de juridische kaders wordt, naar aanleiding van het rapport van de Commissie Dessens[6], door het kabinet bezien hoe de Wet op de Inlichtingen en Veiligheidsdiensten (Wiv2002) op zowel het gebied van privacy als de (technische) bevoegdheden geactualiseerd kan worden.

---

[6] Evaluatie Wet op de Inlichtingen en Veiligheidsdiensten 2002, Commissie Dessens, 2-12-2013

Versterking civiel-militaire samenwerking

Militaire en civiele actoren zijn in het digitale domein steeds meer met elkaar verweven. Een civiel-militaire aanpak ter vergroting van de digitale veiligheid is daarom noodzakelijk. In 2014 zijn forse stappen gezet in de opbouw van Defensie cybercapaciteiten. Zo zijn operationele capaciteiten versterkt en is in oktober 2014 het Defensie Cyber Commando opgericht van waaruit de Defensie cyberactiviteiten worden aangestuurd en gecoördineerd. In 2014 is tevens het Defensie Cyber Expertise Centrum (DCEC) opgericht voor kennisontwikkeling, opleiding van het personeel, innovatie en onderzoek. Tevens wordt een doctrine opgesteld voor de inzet van cybercapaciteiten in militaire operaties. Recent is de Defensie Cyber Strategie geactualiseerd. Deze strategie geeft de komende jaren richting aan de doorontwikkeling van cybercapaciteiten bij Defensie. Eerder dit jaar heeft de Minister van Defensie besloten om structureel meer geld voor cyber beschikbaar te stellen en hiermee een aanzet gegeven tot de noodzakelijke doorontwikkeling van het inlichtingenvermogen en operationele cybercapaciteit. Met het oog op de beschikbaarheid van voldoende gekwalificeerd personeel in het geval van cyberincidenten is in 2014 een Defensie cyberreservistenbestand opgericht. Dit bestand wordt momenteel gevuld.

Tussen het Ministerie van Veiligheid en Justitie en het Ministerie van Defensie is regulier en nauw contact over de ontwikkeling van cybercapaciteiten en het vormgeven van de civiel-militaire samenwerking. Om de samenwerking te faciliteren zijn in 2014 wederzijdse detacheringen van functionarissen van de NCSC en het Defensie Cyber Commando overeengekomen. Daarnaast heeft de samenwerking tussen DefCERT en het NCSC een permanente en formele status gekregen met het ondertekenen van een samenwerkingsconvenant.

Versterking Nationaal Cyber Security Centrum (NCSC)

De in 2014 ingezette personele versterking van het NCSC heeft in 2015 verder vorm gekregen. Met het 24/7 beschikbare Nationaal Cyber Security Operations Center (NCSOC) functioneert als meldpunt, signaleert nieuwe dreigingen en voorziet haar netwerk van contacten van opvolgbare informatie. Het NCSOC moet, met hulp van het Nationaal Detectie Netwerk (NDN), gaan zorgdragen voor het situationeel beeld ten aanzien van cyberdreigingen. Het NDN is een samenwerkingsverband, waarbinnen NCSC, AIVD en MIVD gezamenlijk met andere overheids- en marktpartijen optrekken, om de vroegtijdige detectie van cyberdreigingen te faciliteren. In 2014 is het basisnetwerk ontwikkeld en gerealiseerd dat in 2015 en verder uitgebouwd zal worden. De werking van het NDN is aanvullend op de eigen detectie-inspanningen van de organisaties. Het NDN sluit aan op het eveneens publiek-private Nationaal Respons Netwerk (NRN) dat, onder de coördinatie van het NCSC, de gezamenlijke respons op cybersecurity-incidenten versterkt.

Als onderdeel van de verdere professionalisering van het NCSC is de Inspectie voor Veiligheid en Justitie verzocht een onderzoek uit te voeren naar het gebruik van beveiligingsadviezen, ofwel *advisories* van het NCSC. Het volledige onderzoek treft u aan in bijlage 3. De inspectie geeft hierbij aan dat de beveiligingsadviezen in de huidige vorm niet voor alle partijen voldoende meerwaarde bezitten. Doch geeft daarbij aan dat de meerwaarde schuilt in het feit dat de adviezen afkomstig zijn van een onafhankelijke autoriteit met een gezaghebbende positie. Het NCSC kan volgens hen over de commerciële schotten kijken en een objectief advies leveren. In dat kader beveelt de Inspectie het NCSC aan om het product beveiligingsadviezen te heroverwegen en daarbij o.a. aandacht te hebben

voor de gerichtheid van adviezen, de hoeveelheid adviezen en de mate waarin onderliggende informatiebronnen van de advisories reeds voor partijen te ontsluiten zijn. Aan de hand van het inspectierapport zullen de advisories van het NCSC in het komende jaar verder worden doorontwikkeld teneinde te blijven voorzien in een voor publieke en private partijen relevant product.

Legacysystemen, toezicht en accreditatie

In 2015 heeft het NCSC een methodiek ontwikkeld om de risico's voor legacysystemen binnen de vitale infrastructuur in kaart te brengen. Deze zal eind november tijdens de jaarlijkse Alert Online campagne worden gepubliceerd en onder de aandacht worden gebracht van organisaties in de vitale infrastructuur.

Een effectief cybersecurity toezicht is één van de speerpunten in de komende EU-richtlijn voor Netwerk- en Informatiebeveiliging waarvoor momenteel de onderhandelingen in volle gang zijn. Het bestaande sectorale toezichtinstrumentarium zal eind 2015 in kaart zijn gebracht. Bij de implementatie van de EU-richtlijn zal een versterking van het Nederlandse toezichtinstrumentarium op cybersecurity vorm krijgen. Tenslotte is in 2015 een verkenning gestart naar diverse internationale accreditatiesystemen voor bedrijven die als «digitale brandweer» kunnen optreden. Deze verkenning wordt eind 2015 afgerond.

Internationale aanpak cybercriminaliteit

Cybercrime is naast cyberspionage de andere grote dreiging op het gebied van cybersecurity. Om de aanpak van cybercrime stevig aan te pakken wordt de (straf)wetgeving versterkt. Hiertoe is het wetgevingstraject voor de wet computercriminaliteit III ingezet. De wet computercriminaliteit III geeft de politie meer slagkracht voor de opsporing in cyberspace. Internationaal wordt ingezet op het versterken van de samenwerking en het harmoniseren van wetgeving. Daarom is het thema cybercrime op de agenda van de GCCS2015 geplaatst en op de agenda van het Nederlandse EU voorzitterschap in 2016. Ook zet Nederland zich onverminderd in voor de discussie in het kader van het Cybercrimeverdrag bij de Raad van Europa. De nationale beleidsdoelstelling ten aanzien van de aanpak van cybercrime is een verbreding van de aanpak van high tech crime zaken op het niveau van de landelijke eenheid naar de aanpak van cybercrime op het niveau van alle eenheden van politie. In de Veiligheidsagenda 2015–2018 is vastgesteld dat het aantal cybercrimezaken groeit naar totaal 360 zaken in 2018. De afgesproken aantallen laten een duidelijke stijgende lijn zien.

Op operationeel niveau heeft de politie in 2014 een personele versterking van onderzoeks- en analysecapaciteiten gerealiseerd doordat het Team High Tech Crime (THTC) van politie op sterkte is gekomen, namelijk 119 fte. Voor de komende periode is de aandacht daarom gericht op het verruimen van de aanpak van high tech crime zaken op het niveau van de landelijke eenheid naar de aanpak van cybercrime op het niveau van alle eenheden van de politie. Een randvoorwaarde daarvoor is het versterken van de digitale expertise. In 2015 is gestart met het (extern) werven van digitaal specialisten. Ook is geïnvesteerd in de benodigde technische ondersteuning en zijn standaarden vastgelegd en geïmplementeerd.

Naast deze specialistische ondersteuning wordt ingezet op bewustwording en toerusting van alle medewerkers om de benodigde bijdrage aan de aanpak van cybercrime en gedigitaliseerde criminaliteit te kunnen leveren. Zo zijn er handreikingen opgesteld (voor de intake van cyber-

crime en het betreden van een plaats delict in een gedigitaliseerde omgeving) en is de ambitie om het trainings- en opleidingsaanbod op dit thema uit te breiden.

Internationaal is een intensieve samenwerking tot stand gekomen met het European Cyber Crime Centre van Europol. Dit centrum versterkt de samenwerking tussen Europese politieorganisaties en faciliteert de contacten met landen buiten Europa. Bovendien is het nieuwe Interpol Global Complex for Innovation (IGCI) in Singapore in april officieel geopend. Het IGCI ondersteunt politieorganisaties wereldwijd in de bestrijding van innovatieve vormen van criminaliteit. Voor de bestrijding van cybercrime is het IGCI van groot belang. De Nederlandse politie heeft er inmiddels medewerkers gedetacheerd.

Cyberdiplomatie: kennis en capaciteitsopbouw

Het internationale karakter van cybersecurity kwam nadrukkelijk naar voren bij de GCCS 2015 waarvan Nederland gastheer was op 16 en 17 april dit jaar. Deze internationale top met vertegenwoordigers op ministerieel niveau, van internationale organisaties en leiders uit de private sector benadrukte het belang van internationale samenwerking tussen alle stakeholders en kennisuitwisseling in het digitale domein. Door internationaal samen te werken kunnen dreigingen worden aangepakt en kansen van het digitale domein optimaal worden benut. Nederland heeft met de top laten zien dat het haar rol als bruggenbouwer ook in het digitale domein kan vervullen.

Het onderwerp vrijheid en privacy is door Nederland toegevoegd aan de agenda van de GCCS. Dit is in lijn met de Nederlandse visie dat allen gebaat zijn bij een internet dat vrij, open en veilig is. Conform de Chair's Statement van de GCCS, zal Nederland zich blijven inzetten voor het versterken van de rol van mensenrechten in het cyberdebat om zeker te stellen dat cybersecurity beleid zoveel mogelijk in overeenstemming is met verplichtingen die voortvloeien uit mensenrechtenverdragen. Tijdens de GCCS heeft Nederland zich ook nadrukkelijk ingezet om alle stakeholders volwaardig te betrekken bij het debat. Deze inspanningen om multistakeholder deelname in het cyberdebat te vergroten zal Nederland voortzetten in de komende periode. Zo zal Nederland projecten ondersteunen die gericht zijn op het faciliteren van effectieve deelname van civil society aan debatten zoals de WSIS+10 Review Process en het Internet Governance Forum.

Nederland zet in op het duurzaam stimuleren van cybercapaciteitsopbouw in internationaal verband, zowel in minder cyber-ontwikkelde landen als in landen waar het cyberdomein relatief ver ontwikkeld is. Het gaat daarbij om het delen van kennis en expertise op een aantal centrale cyberthema's tussen internationale publieke en private partners. Het belangrijkste instrument daarvoor is het, tijdens de GCCS gelanceerde, mondiale Global Forum on Cyber Expertise (GFCE). Het GFCE is een concreet initiatief van landen, bedrijven en intergouvernementele organisaties om door middel van capaciteitsopbouw brede inspanning te doen op het gebied van cybersecurity. Naast cybersecurity draagt het platform ook bij aan de strijd tegen cybercrime, het verbeteren van databescherming en het versterken van e-governance. De oprichting van het GFCE is een belangrijke stimulans om wereldwijd verder te werken aan capaciteitsopbouw in het digitale domein. Dankzij het platform zal technische expertise breder gedeeld kunnen worden en zullen kennis en middelen ter beschikking worden gesteld voor het versterken van cybersecurity. Het GFCE Secretariaat zal voor de komende vier jaar in Den Haag gevestigd zijn. Daarnaast zal Nederland zich inzetten om actief gebruik te maken van

de kennis en expertise van non-gouvernementele organisaties, wetenschap en de technische gemeenschap om de publieke kern van het internet te waarborgen.

De internationale visie van de Nationale Cyber Security Strategie 2 gaat uit van een geïntegreerde aanpak, waarin naast het belang van *defence* en *development*, in de vorm van capaciteitsopbouw, ook middels *diplomacy* wordt bijgedragen aan meer stabiliteit in het cyberdomein. Cyberdiplomatie wordt daarbij enerzijds ingezet als ondersteunend instrument tijdens crisisbeheersing en respons op cyberincidenten op de korte termijn en anderzijds voor het op middellange termijn bewerkstelligen van een internationaal normatief kader voor de regulering van cyberoperaties tussen staten. In dat kader heeft Nederland een omvangrijke bijdrage geleverd aan het bereiken van consensus over gedragen normen voor verantwoordelijk Statelijk gedrag en het verhelderen van de toepassing van het internationaal recht in cyberspace. In dat kader zijn inclusieve projecten voor internationale discussie gelanceerd, zoals bijvoorbeeld ten behoeve van de aankomende Tallinn Manual over internationaal recht en cyberoperaties in vredestijd en de International Law and State Behavior in Cyberspace Regional Meeting Series met het United Nations Institute for Disarmament Research.

Nederland heeft ook een vooruitstrevende rol gespeeld in het verder vormgeven en implementeren van vertrouwenwekkende maatregelen, bijvoorbeeld in de OVSE. Deze kunnen een bijdrage leveren aan het vergroten van de internationale stabiliteit en aan het voorkomen van escalatie van cyberconflicten. Hierbij kan gedacht worden aan het opstellen van consultatiemechanismen en contactpunten, het voeren van formele en informele dialogen, het versterken van de contacten tussen Computer Emergency Respons Team's (CERT's) en het delen van nationale cyberstrategieën, doctrines en informatie over de aanpak van cyberincidenten.

Cybersecurity onderwijs

In 2015 is een stevige impuls gegeven aan de acties op het gebied van onderwijs uit de NCSS-2. Gelet op het belang van een veilige digitale omgeving wordt de noodzaak van voldoende cybersecurityspecialisten breed onderschreven. Zo maakt de beroepsgroep cybersecurityspecialisten onderdeel uit van de Human Capital Agenda die door het Ministerie van Economische Zaken wordt ontwikkeld[7]. Cybersecurityspecialisten is een van de doelgroepen waar de acties uit de HCA ICT-innovatie zich op richten.

Het WODC heeft onderzoek gedaan naar de vraag naar diverse soorten werknemers die een rol spelen bij cybersecurity en het aanbod aan onderwijs waarlangs deze worden opgeleid en om/bijgeschoold. Op 1 mei 2015 is de Kamer hierover geïnformeerd[8].
Dit onderzoek stond mede aan de basis van het, in de cybersecurity strategie aangekondigde, Cyber Security Research & Education platform (CSRE-platform). In september jl. is in afstemming met VenJ, OCW, EZ en NWO besloten om de kwartiermakers fase van dit platform te starten. De kwartiermakers fase zal naar verwachting in januari 2016 zijn afgerond waarna het platform definitief zijn beslag krijgt. Het platform heeft als taak de resultaten uit de onderzoeken op het terrein van cybersecurity te delen, met alle betrokkenen in de sectoren bedrijfsleven, overheid en wetenschap/onderwijs. Verder wordt er door het platform een geactuali-

---

[7] https://zoek.officielebekendmakingen.nl/stcrt-2014–28095.html
[8] Kamerstuk 26 643, nr. 613

seerd overzicht gegeven van de cybersecurity leergangen. Zo is bijvoorbeeld naast de reeds bestaande academische bachelor opleiding computer security van de Radboud Universiteit, in 2014 de Cyber Security Academie opgericht door de Hague Security Delta, die een postdoctorale masteropleiding cybersecurity verzorgt en wordt in 2015 door de technische universiteit van Eindhoven en de Radboud Universiteit de masteropleiding Cyber Security aangeboden. Ook is in het middelbaar beroepsonderwijs inmiddels met steun vanuit het Regionaal investeringsfonds mbo een Cyber Security Centre van start gegaan voor het mbo in de regio Amsterdam. Doel is om met deze publiek-private samenwerking o.a. de ICT opleidingen en daarbij behorende stages inhoudelijk te verbreden en te verrijken met alle aspecten van cybersecurity, afgestemd op de kwalitatieve en kwantitatieve vraag naar ICT medewerkers. Daartoe vindt intensieve regionale afstemming, kennisdeling en samenwerking plaats tussen het bedrijfsleven, het vmbo, mbo en hbo op het gebied van cybersecurity.

Stimuleren van innovatie in cybersecurity

Om innovatie in cybersecurity te stimuleren krijgt onderzoek een impuls en zijn vanaf 2012 een tweetal onderzoek tenders uitgevoerd onder de Nationale Cyber Security Research Agenda (NCSRA). De tenders, met een totale omvang van ca. € 11 mln., bestaan voor ca. de helft uit fundamenteel onderzoek (NWO), waar de wetenschap voortouw heeft en bedrijfsleven betrokken moet zijn, en voor de helft uit toegepast onderzoek (SBIR), waar het bedrijfsleven de trekker is en kennisinstituten betrokken zijn. Bij de onderzoektenders (SBIR/NWO) zijn ca. 110 tot120 bedrijven en ca. 50 kennisinstituten betrokken geweest. Rond deze tenders heeft op verschillende momenten kennisuitwisseling (overheid, bedrijfsleven, kennisinstituten) plaats gevonden. Met de opgedane ervaringen wordt thans een vervolgtender vorm gegeven. Tijdens het NCSRA-Symposium op 2 november 2015 worden de onderzoeksprojecten gepresenteerd die binnen de kaders van de NCSRA worden uitgevoerd.